Systematic Cryptographic Reductions Using Bi-Deduction

Justine Sauvage*[1]

[1]Unknown Labs [Inria] – L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France

Abstract

The formal verification of security protocols is a notoriously important and complex problem. In this talk, we are interested in
the Computationally Complete Symbolic Attacker (CCSA) approach to this problem, which builds on logics whose terms are interpreted as probabilistic computations representing the messages exchanged by a protocol interacting with an arbitrary attacker, and which is notably implemented in the proof assistant Squirrel.
The CCSA logics come with cryptographic axioms, which are crucial to prove security properties of protocols, and whose soundness derives from the security of standard cryptographic games, e.g. PRF, EUF, IND-CCA.
Unfortunately, these axioms are complex to design and implement; so far, these tasks are manual, ad-hoc and error-prone.
We solve these issues by providing a formal and systematic method for deriving axioms from cryptographic games.
Our method relies on synthesizing (parts of) an adversary w.r.t. some cryptographic game, through the notion of bi-deduction.
In addition to defining a rich notion of bi-deduction and justifying how cryptographic axioms derive from it, we provide a proof system for establishing bi-deduction, an automatic proof-search method for it, and we implement it in an extension of Squirrel.

*Speaker